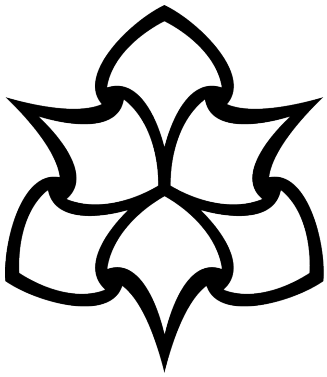


Cybersecurity Measures for Geocasting in Vehicular Cyber Physical System Environments

Sushil Kumar, *Member IEEE*, Upasana Dohare, Kirshna Kumar, Durga Prasad, Kashif Naseer Qureshi, *Member IEEE*, Rupak Kharel, *Senior Member IEEE*

***Abstract*- Geocasting in vehicular communication has witnessed significant attention due to the benefits of location oriented information dissemination in vehicular traffic environments. Various measures have been applied to enhance geocasting performance including dynamic relay area selection, junction nodes incorporation, caching integration, and geospatial distribution of nodes. However, the literature lacks towards geocasting under malicious relay vehicles leading to cybersecurity concern in vehicular traffic environments. In this context, this paper presents Cybersecurity Measures for Geocasting in Vehicular traffic environments (CMGV) focusing on security oriented vehicular connectivity. Specifically, a vehicular intrusion prevention technique is developed to measure the connectivity between the cache agent and cache user vehicles. The connectivity between static transport vehicles and cache agent/cache user is measured via vehicular intrusion detection approach. The performance of the proposed vehicular cybersecurity measure is evaluated in realistic traffic environments. The comparative performance evaluation attests the benefits of security oriented geocasting in vehicular traffic environments.**

Index Terms—Geocasting, Vehicular ad-hoc networks, Vehicle cybersecurity, Caching

I. Introduction

LOCATION oriented decision making in driverless cars is one of the finest examples of the significance of location oriented communication in vehicular cyber physical systems environments (see Fig. 1) [1, 2, 3]. The location-oriented services in vehicular environments is continuously growing staring from navigation to real time traffic prediction. It includes smart use cases of intelligent transport system such as safety and efficiency oriented cooperative vehicular communication, and sensor oriented emergency response for driver assistance [4, 5]. Recently, location oriented vehicular communication also known as geocasting has witnessed significant attention considering its applicability in the wide range of ITS applications [6].

S. Kumar, U. Dohare and K. Kumar are with Jawaharlal Nehru University (JNU), New Delhi, 110067, India. Email: {skdohare@mail.jnu.ac.in, upasanadohare@yahoo.com, kirshn44_scs@jnu.ac.in}

D. P. Dora is with Central University of Himachal Pradesh, 176206, India. Email: doradurga@gmail.com

KN. Qureshi is with Department of Computer Science, Bahria University, Islamabad, Pakistan, Email: knaseer.buic@bahria.edu.pk

R. Kharel (Corresponding Author) is with the School of Engineering, Manchester Metropolitan University, M1 5GD, UK Email: r.kharel@mmu.ac.uk

Location oriented vehicular communication has been extensively explored for performance improvements focusing on vehicle mobility management. A geocasting technique has been presented focusing on locality centric regular vehicles as information caching points during opportunistic transmissions [7]. It has developed a dynamic transmission range adaptation enabled caching technique for addressing intermittent connectivity in urban vehicular traffic environments. However, the caching centric geocasting is far from addressing malicious caching vehicles in traffic environments. The segment vehicle, link quality, and degree of connectivity oriented performance improvement in geographic information dissemination has been suggested for vehicular traffic environments [8]. The relay vehicles have been selected within the dynamic segment area of the transmission range. The selection has been aided using the information about quality of link, and degree of connectivity, with the corresponding next cell of transmission for each vehicle within segment area. However, the segment vehicle oriented performance improvement lacks malicious segment vehicles consideration. A mobility immune geographic information dissemination technique has been suggested suitable for opportunistic vehicular networks [9]. It has identified information dissemination trajectory from source to destination focusing on mobility immune characteristic of the trajectory. It has utilized a multi-queueing system for prioritizing data transmission during opportunistic node encounters. The mobility immune geographic information dissemination also lacks considering malicious mobile nodes environments and its security oriented implications.

The cybersecurity on location centric information dissemination lacks volume in literature under vehicular traffic environments. Location centric malicious vehicle detection has been investigated considering single and multiple location (path) forging of vehicles as case studies [10]. The malicious vehicles detection strategy is based on the transmission range and speed variance monitoring via roadside units infrastructure. The deployment constraints of roadside infrastructure reduces the feasibility considering financial and planning aspects. To overcome the infrastructure constraint, directional antenna based location verification system has been suggested without depending on roadside units [11]. The multiple directional antennas have been utilized for preprocessing received signal strength values of the location claim of vehicles. The claim has been further verified using a static wireless location verification system. The number of directional antenna requirement reduces the applicability and generalization of the technique. Towards reducing the directional antenna constraint, a location verification oriented security framework has been suggested for geographic information dissemination [12]. The two levels of

security filter has been presented for detecting malicious vehicle focusing on link quality in initial level, and statistical accumulation of neighbor belief in second level. However, the aforementioned location verification oriented vehicular security approaches are more suitable for non-critical traffic applications, rather than location oriented information dissemination or geocasting. More provable security approach than verification is the need of the hour for location centric information dissemination in vehicular traffic environments.

Towards this end, this paper presents a framework for Cybersecurity Measures for Geocasting in Vehicular traffic environments (CMGV) focusing on security oriented vehicular connectivity. It consists of vehicular intrusion prevention and, detection techniques against cyberattacks in connected vehicle environments. The vehicular cybersecurity framework is implemented for location oriented information dissemination or geocasting to test its resistive performance against malicious vehicles. The key contributions of the paper can be summarized as follows:

1) Firstly, a system model for the vehicular cybersecurity connectivity is presented focusing on expectation of the presence of the nearest security authenticator and the probability of connectivity.
2) Secondly, a vehicular intrusion prevention (VIP) technique is proposed using two-way authentication at network initialization stage namely, cache-user side authentication and cache-agent side authentication.
3) Thirdly, a vehicular intrusion detection technique is developed focusing on next hop verification using unauthorized node detection and compromised node detection.
4) Finally, the proposed vehicular security framework CMGV is tested to comparatively evaluate the performance with state-of-the-art techniques focusing on network performance and security related metrics under vehicular traffic environments.

The rest of the paper is organized as follows. Section II reviews the recent unsecure and security oriented geocasting techniques for vehicular networks. Section III presents the detail of the proposed vehicular cybersecurity measures for geocasting in vehicular traffic environments. Section IV discusses simulation setting and analysis of results. Section V presents conclusion and future direction of the work.

II. Related Work

In this section, related literature on data propagation in VANETs has been reviewed focusing on unsecured geocasting and security-based geocasting.

A. Unsecured Geocasting

Caching and transmission range control (CTRC) based geocast routing utilizes two forwarding schemes: line forwarding for hop- to- hop data delivery and area forwarding for hop-to-multi hop data delivery [13]. Range forwarding reduces the transmission range. For that reason the effect of dynamic mobility patterns and speed of vehicular nodes on data delivery ratio is greatly reduced. It also increases hop count drastically. The metrics: segment vehicle, link quality and degree of connectivity have been utilized to select next hop vehicle in vehicular adhoc networks [8]. Although it reduces one hop disconnection, yet increases hop count. . However, the segment vehicle oriented performance improvement lacks malicious segment vehicles consideration. Guaranteed geocast routing has been suggested to provide reliable packet forwarding based on caching and heuristic function in intermittently connected vehicular environment [7]. It minimizes the hop to hop disconnection, hop count and end to end delay in non-malicious environment while lacking performance in malicious environment. Multi-metric geographical routing has been proposed to select next hop vehicle from dynamic forwarding region while considering future position of vehicle, received signal strength and critical area vehicles as forwarding metrics [14]. It reduces end to end delay, hop count and probability of link failure while maintaining quality of connectivity. In case of integration with traffic light and real time traffic status, performance is degraded.

Cache agent based geocast (CAG) routing has been suggested while categorizing vehicles as cache agent (CA) and cache user (CU) [15]. When a CU leaves its old locality and enters into a new locality, the incumbent CA sends its presence information. Connectivity assurance algorithm (CAA) is utilized to assure successful delivery of cached data. Despite of transmitting data packets with full radio range, probability of connectivity drastically reduces in case of attack by intruders. The static cache used in CAA, causes resource wastage. The issue of reachability is also a big concern. It only retransmits when cached data is not successfully delivered to the notified target node. A mobility immune geographic information dissemination technique has been suggested suitable for opportunistic vehicular networks [9]. It has identified information dissemination trajectory from source to destination focusing on mobility immune characteristic of the trajectory. It has utilized a multi-queueing system for prioritizing data transmission during opportunistic node encounters. The mobility immune geographic information dissemination also lacks considering malicious mobile nodes environments and its security oriented implications. The channel selection framework based on fuzzy has been suggested for location oriented services in multichannel vehicular cyber physical system [16]. Channel access delay which is derived using Markov chain model, and signal to interference ratio are utilized to estimate channel quality. It minimizes the problem of traffic imbalance and end to end delay and enhances throughput. Still, this approach does not incorporate dynamic node mobility patterns. For that reason, its efficiency is not accurately gauged in VANETs. Connectivity-aware routing (CAR) has been explored while utilizing path segments with higher probability of connectivity [17]. The probability of connectivity is derived from probabilistic model of network disconnection and uses statistical traffic information. In case of inaccurate road density calculation, estimation of optimized path selection can be inaccurate.

B. Security Oriented Geocasting

Location centric malicious vehicle detection has been investigated considering single and multiple location (path) forging of vehicles as case studies [10]. The malicious vehicles detection strategy is based on the transmission range and speed

variance monitoring via roadside units infrastructure. The deployment constraints of roadside infrastructure reduces the feasibility considering financial and planning aspects. To overcome the infrastructure constraint, directional antenna based location verification system has been suggested without depending on roadside units [11]. The multiple directional antennas have been utilized for preprocessing received signal strength values of the location claim of vehicles. The claim has been further verified using a static wireless location verification system. The number of directional antenna requirement reduces the applicability and generalization of the technique. Towards reducing the directional antenna constraint, a location verification oriented security framework has been suggested for geographic information dissemination [12]. The two levels of security filter has been presented for detecting malicious vehicle focusing on link quality in initial level, and statistical accumulation of neighbor belief in second level.

Location error resilient geographical routing has been suggested to assess error in the neighboring vehicle's location while utilizing error estimation technique based on Rayleigh distribution [18]. The neighboring vehicle's location is predicted using location prediction and correction technique based on Kalman filter. The route reporting scheme while preserving privacy has been proposed for both self-organizing and infrastructure based traffic management systems [19]. In this scheme, two variants of route sharing: elliptical curve cryptography point addition based route sharing scheme and homomorhic encryption based route sharing scheme have been suggested for self-organizing vehicular ad hoc network. An information theoretic framework for location verification has been developed while minimizing mutual information between input and output data of system [20]. In this framework, input data is taken as user's claimed location and base station received signal strength, while forming optimal decision rules. Non line of sight location verification scheme has been suggested among cooperative neighboring vehicles while securing integrity for localization services in vehicular environment [21]. The false location advertising malicious vehicle detection has been investigated using proactive cooperative neighbor location verification scheme [22]. It avoids malicious vehicle to forward critical information by utilizing two warning dissemination techniques in vehicular environment.

In [23, 24], Public Key Infrastructure (PKI) model based on asymmetric cryptography has been proposed to protect VANETs from outside attacks. But, it is unable to detect the inside attacks. A novel model, simpler and cheaper than PKI based system utilizes two techniques for data dissemination: directional data verification and time based data verification [25]. The critical data has been disseminated through two channels and information received from both channels has been verified by the recipient vehicles to check integrity.

III. Vehicle Cybersecurity Measures for Geocasting

In this section, the proposed Cybersecurity Measures for Geocasting in Vehicular traffic environments (CMGV) is presented in detail. It consists of system model for connectivity oriented vehicular cybersecurity, vehicular intrusion prevention, and vehicular intrusion detection.

Table I. Notations

Notation	Description	Notation	Description
R_1	Transmission range of CA	x_{ln}	Longitude
R_2	Transmission range of CU	x_{lt}	Latitude
r	Euclidean distance	t_s	Timestamp
E	Expectation	P	Probability
$f_r(r)$	Probability density function	p_u	Public key
$E(r)$	Expected distance	p_v	Private key
P_{CA}^c	Probability of connectivity of CA	g	Very large prime number
P_{SV}^c	Probability of connectivity of SV	r_v	Verification component
V_n	Number of vehicles	m_v	Validation component
λ	Density of vehicles	x	GPS location of vehicle

A. System Model-Vehicular Cybersecurity Connectivity

A realistic vehicular traffic environment is considered for connectivity oriented vehicular cyber security measurements. The vehicular infrastructure is based on cache agent[1] (CA), cache user[2] (CU) and static vehicular infrastructure[3] (SV) consideration. Vehicles of particular locality or junction having some predefined source and destination are considered as CA, while other vehicles not belonging to this category are considered as CU. Roadside transmission unit and other infrastructure are considered as SV. The cache agent vehicles execute distributed authentication and provide local caching support in case of disconnected vehicular network environments. The cache user vehicles executes cooperative location oriented information dissemination or geocasting. The cache users eliminates malicious vehicles while geocasting via vehicular intrusion prevention and detection. The static vehicular infrastructure executes alternative security verification for cache user and cache agent vehicles in case of network load oriented delay in vehicular security verification.

A vehicle v_i execute the cybersecurity framework on either nearest CA or SV. Here, the distance between the nearest CA or SV and v_i is quite significant and must be less than R for maintaining connectivity to execute the framework. The probability $P_{r|(r+\Delta r)}^{n_{CA/SV}}$ of the presence of a nearest CA or SV is a join probability as expressed in Eq. (1).

$$P_{r|(r+\Delta r)}^{n_{CA/SV}} = P_{<r}^{0} \times P_{r|(r+\Delta r)}^{s_{CA/SV}} = \left[1 - P_{<r}^{s_{CA/SV}}\right] \times \left[P_{r|(r+\Delta r)}^{s_{CA/SV}}\right] \quad (1)$$

Where $P_{<r}^{0}$ represents the probability of no CA or SV at a distance smaller than $r < R$, $P_{r|(r+\Delta r)}^{s_{CA/SV}}$ denotes the probability of some CA or SV between the distances r and $(r + \Delta r)$, and $P_{<r}^{s_{CA/SV}}$ represents the probability of some CA or SV at a distance smaller than r. Towards directional authenticator searching, front half of the transmission range is considered in Eq. (1) for further simplification as given by Eq. (2).

$$P_{r|(r+\Delta r)}^{n_{CA/SV}} = \left[1 - \sum_{j=1}^{V_n} \binom{V_n}{j} \left(\frac{\lambda\pi r^2}{2}\right)^j \left(1 - \frac{\lambda\pi r^2}{2}\right)^{V_n - j}\right] \times \left[\sum_{j=1}^{V_n} \binom{V_n}{j} \int_r^{r+\Delta r} \left(\frac{2\lambda\pi r\, dr}{2}\right)^j dr . \int_r^{r+\Delta r} \left(1 - \frac{2\lambda\pi r\, dr}{2}\right)^{V_n - j} dr\right]$$

$$= (1-\lambda\pi r^2)^{V_n}\left[V_n\,\lambda\pi r dr + V_n\lambda\pi dr^2 - \binom{V_n}{2}.\left(\lambda\pi(rdr + dr^2)\right)^2 \ldots\right] \quad (2)$$

Where V_n represents the number of vehicles in network area, and λ is the density of vehicles. By applying limit theorem in Eq. (2), the probability density function $f_r(r)$ of the distance of the nearest CA or SV is derived as given by Eq. (3).

$$f_r(r) = \lim_{dr\to 0}\frac{P_{r|(r+\Delta r)}^{n_{CA/SV}}}{dr} = V_n\lambda\pi r(1-\lambda\pi r^2)^{V_n} \quad (3)$$

By utilizing Eq. (3) with restricted network area V_A, the expected distance of the nearest CA or SV can be derived as expressed in Eq. (4).

$$E(r) = \int_0^R r f_r(r)dr = \int_0^R r V_n\lambda\pi r(1-\lambda\pi r^2)^{V_n}dr$$
$$= \left[\frac{1}{\lambda\pi(V_n+1)}\sum_i^{V_n+1}\binom{V_n+1}{i}\frac{(-\lambda\pi r^2)^i\, r}{i+1}\right]_0^R$$
$$= \frac{\sqrt{V_A}}{\lambda\pi^{3/2}(V_n+1)}\sum_i^{V_n+1}\frac{(-1)^i}{i+1} \quad (4)$$

The constraint $E(r) < R$ related to the expected distance $E(r)$ and transmission R is significant for the successful execution of the vehicular cybersecurity framework. Once the aforementioned constraints satisfies, the connectivity between the target vehicles with either CA or SV is another major service monitoring parameter. Towards verifying the probability of connectivity, let us consider the arrival rate of vehicular nodes on road follows Poisson process and the inter-arrival time is exponentially distributed with parameter ρ. It is also assumed that there are N discrete levels of speed of vehicles in the network, i.e. $s_1, s_2, s_3 \ldots s_N$. The probability P_{CA}^c of connectivity with CA can be expressed as given by Eq. (5).

$$P_{CA}^c = \begin{cases} P_{r|(r+\Delta r)}^{n_{CA}}, E(r) < R \\ P_{r|(r+\Delta r)}^{n_{CU}} \times P_{r|(r+\Delta r)}^{n_{CA/SV}}, otherwise \end{cases} \quad (5)$$

Where $P_{r|(r+\Delta r)}^{n_{CU}}$ is the probability of the presence of a CU which is further connected to CA or SV in the next hop transmission. Similarly the probability P_{SV}^c of connectivity with SV can be derived as given by Eq. (6).

$$P_{SV}^c = \begin{cases} P_{r|(r+\Delta r)}^{n_{SV}}, E(r) < R \\ P_{r|(r+\Delta r)}^{n_{CU}} \times P_{r|(r+\Delta r)}^{n_{CU/SV}}, otherwise \end{cases} \quad (6)$$

By utilizing Eq. (5) and (6), the probability $P_{CA/SV}^c$ of successful execution of the security framework can be calculated as normalized probability.

B. Vehicular Security Measures

1) Vehicular Intrusion Prevention

In the vehicular intrusion prevention (VIP), authentication is performed at both cache user, cache agent sides. The authentication ensure security oriented connectivity between cache agent and cache user in one and multi hops communications. The transmission range of cache users and cache agents are managed dynamically towards reducing error insertion and further propagation. It is developed as two authentication process namely, cache user side and cache agent side authentication.

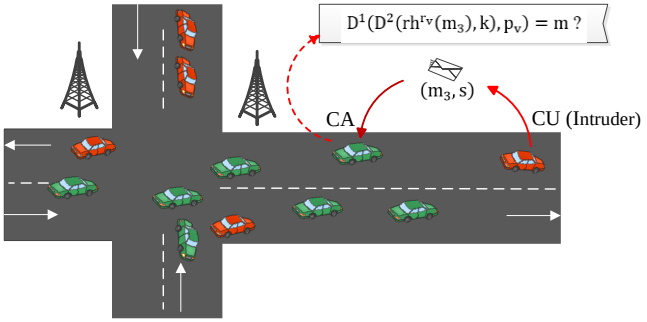


Fig. 1. Vehicular Intrusion Prevention

Algorithm 1: Vehicular Intrusion Prevention

Input: x_{lt}, x_{ln}, t_s, m;
Process:
1. Extract x_{lt}, x_{ln}, and time stamp t_s attached with a cache user.
2. Cache User side Autentication (x_{lt}, x_{ln}, t_s, m)
   The cache user generates the public key p_u, and the private key p_v.
3. Broadcasts the key p_u to neighboring vehicles.
4. Generates a large prime number g
5. Calculate $k = x_{lt}^{x_{ln}}$ and $r = g^{p_u k \ln k}$
6. Encrypts the message m using the Eq. (7) into the message m_3.
7. Calculates $s = p_u \times k \times \ln(m_3 \times k)$
8. Transmit (m_3, s) message to the intended cache agent inside the cache user's cluster.
9. **end** Cache User side Autentication ()
10. Cache Agent side Authentication (p_u, (m_3, s))
11. The cache agent generates a private key $p_v = g^{p_u}$.
12. Calculates verification component r_v using Eq.(8)
13. **if** ($r_v = r$) **then**
14. Calculates validation component m_v using Eq. (9).
15. **if** ($m_v = m$) **then**
16. The cache agent validates the message m
17. **else** message m is altered.
18. **end if**
19. **else** Discard m;
20. **end if**
21. **end** Cache Agent side Authentication ()

In cache-user side authentication, a cache user carries out authentication before disseminating any data packets in the network among cache agents. The authentication is performed in three phases including setup, key generation and signing. In the setup phase, spatiotemporal data such as latitude x_{lt}, and longitude x_{ln} of a GPS location x, and time stamp values attached with cache user are extracted and passed it as parameters to the next key generation phase. In key generation, each cache user generates a public key p_u and private key p_v. Further, the public key is disseminated among the neighboring cluster vehicles. In the signing phase, the cache user generates a large prime number g and calculates $k = x_{lt}^{x_{ln}}$ and $r = g^{p_u \times k \times \ln \times k}$. Here, p_u is the public key of the intended cache agent of the cluster in which target vehicle belongs. Further to this, the hashing oriented triple encryption system is applied message m. The three rounds of encryption execution can be expressed as given by Eq. (7).

$$m(m_1, m_2, m_3) = \begin{cases} m_1 = E^1(p_u, m) \\ m_2 = E^2(k, m_1) \\ m_3 = h^r(m_2) \end{cases} \quad (7)$$

Where $E^1$and E^2 represents encryption function and h denotes the hashing function. Further, cache user calculates $s = p_u \times k \times \ln(m_3 \times k)$ and floods (m_3, s) message inside its cluster for disseminating the message to the intended cache agent for authentication (see fig. 1).

In cache-agent side authentication operates in two phases including verification and integrity tests towards ensuring identification of malicious manipulation in received data. The intended cache agent generates its public key p_u and private key $p_v = g^{p_u}$ in key generation phase of cache-user side authentication. The CA initiates verification once it receives (m_3, s) message from neighboring vehicles. In verification, cache agent calculates verification component r_v and compares it with r as expressed in Eq. (8).

$$r_v = \frac{g^s}{p_v{}^{k \ln m_3}} == r = g^{p_u k \ln k} \tag{8}$$

The cache agent moves to integrity phase with the successful verification test in Eq.(8). Towards ensuring malicious altercation identification, cache agent calculates validation component m_v and compares it with m as expressed in Eq. (9).

$$m_v = \begin{cases} D^1(m_1, p_v) == m \\ D^1(D^2(m_2, k), p_v) == m \\ D^1(D^2(rh^{r_v}(m_3), k), p_v) == m \end{cases} \tag{9}$$

Where D^1 and D^2 represents decryption function, rh denotes reverse of the hashing function considered. The cache agent validates the message and moves to further transmission towards the intended cache user vehicle. The complete process of intrusion prevention is presented as Algorithm 1.

2) Vehicular Intrusion Detection

The vehicular intrusion detection (VID) operates towards security enhancements in one and two hop communication between cache agent or cache user and static vehicular infrastructure. Towards identifying malicious error insertion and propagation, VID operates in two phases in vehicular infrastructure supported communication considering the larger transmission range. Firstly, it detects all the unauthorized or unauthenticated vehicles in the vehicular network. Secondly, it detects all the compromised nodes in the vehicular network.

The unauthorized node detection operates as the network initialization phase for new vehicles both cache user and cache agent. It is a cooperative vehicle initialization where the neighboring vehicles or vehicular infrastructure is responsible for authenticating any new or unknown vehicles in the network. Let us consider, a new node X_1 joins the network with existing already authenticated nodes A, B and C (see Fig. 2). The neighboring nodes under direct communication range authenticate in joining the network. Considering node A out of transmission range, the cooperative network initialization of X_1 by the nodes under direct transmission range B and C can be sequentially expressed as given by Eq. (10)-(14).

$$X_1 \to B, C: m_1 = \beta_1{}^{-x_1} \beta_3{}^{x_3} \tag{10}$$

$$B, C \to X_1: m_2 = H(\beta_1, \beta_3, x_1, x_3, m_1) \tag{11}$$

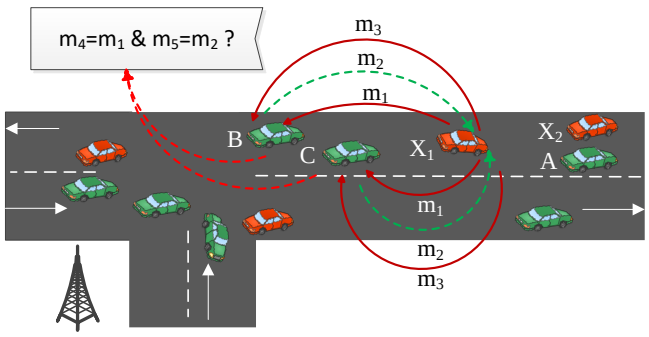


Fig. 2. Vehicular Intrusion Detection

Algorithm 2: Vehicular Intrusion Detection

Input: x_1, x_2, x_3, x_4;
Process:

1. Unauthorized Node Detection (x_1, x_2, x_3, x_4)
2. Authenticate new vehicle by already authenticated neighboring vehicles existing in direct communication range.
3. New vehicle calculates message m_1 using Eq. (10)
4. Neighboring vehicles calculate message m_2 using Eq. (11)
   New vehicle calculates message $m_3$using Eq. (12)
5. Neighboring vehicles calculate message m_4 and m_5 using Eq. (13) and Eq. (14)
6. Neighboring vehicles validate new vehicle using Eq. (15) and Eq. (16)
7. **if** ($m_4 == m_1$&& $m_5 == m_2$) **then**
8. Authorized vehicle
9. **else** Unauthorized vehicle;
10. **end** if
11. **end** Unauthorized Node Detection **()**
12. Compromised Node Detection (x_1, x_2, x_3, x_4)
13. New vehicle calculates message m_1 using Eq. (17) and transmit to neighboring vehicle.
14. Neighboring vehicles calculate massage m_2 using Eq. (18) and transmit to new vehicle.
15. New vehicle calculates message m_3 using Eq. (19) and transmit to neighboring vehicles.
16. Neighboring vehicles calculate message m_4 and m_5 using Eq. (20) and Eq. (21), respectively.
17. Neighboring vehicles validate new vehicle using Eq. (22) and Eq. (23), respectively
18. **if** ($m_4 == m_1$&& $m_5 == m_2$) **then**
19. Uncompromised vehicle;
20. **else** Compromised vehicle;
21. **end** if
22. **end** Compromised Node Detection

$$X_1 \to B, C: m_3 = \alpha_{14} - \alpha_5 + km_2(\alpha_9 - \alpha_{15}) \tag{12}$$

$$B, C: m_4 = e^{m_3} \frac{(\beta_2{}^{x_2} \beta_4{}^{x_4})^{km_2}}{(\beta_1{}^{x_1} \beta_3{}^{x_3})^{km_2}} \tag{13}$$

$$B, C: m_5 = H(\beta_1, \beta_3, x_1, x_3, m_4) \tag{14}$$

Where $m_i, i = 1 \ldots 5$ represents encrypted message using encryption parameters β_i and α_i . These parameters are calculated as shown in Table I, and II (see Appendix). The neighboring nodes B and C authorize network initialization for X_1 once the following two constraints given by Eq. (15) and (16) are satisfied.

$$m_4 = e^{m_3} \frac{(\beta_2{}^{x_2} \beta_4{}^{x_4})^{km_2}}{(\beta_1{}^{x_1} \beta_3{}^{x_3})^{km_2}} == m_1 \tag{15}$$

$$m_5 = H(\beta_1, \beta_3, x_1, x_3, m_4) == m_2 \tag{16}$$

Once the network initialization successfully completes for X_1, It can further helps in initialization of other new nodes joining the network such as X_2. As an illustration of VID, suppose A, B and C are authenticated nodes, and X_1 and X_2 are joining nodes requesting for network initialization (see fig. 2). Considering node X_1 is out of transmission range of A but B, C are moving within its transmission range. Similarly, node X_2 is out of transmission range of $B$and C, but A and X_1 are moving within its transmission range. Firstly, the node X_1 joins the network initialized by neighbors nodes B, C (node A is out of X_1 's transmission range). Secondly, node X_2 joins the network initialized by its neighbors X_1 and A, as B and C are out of transmission range of X_2.

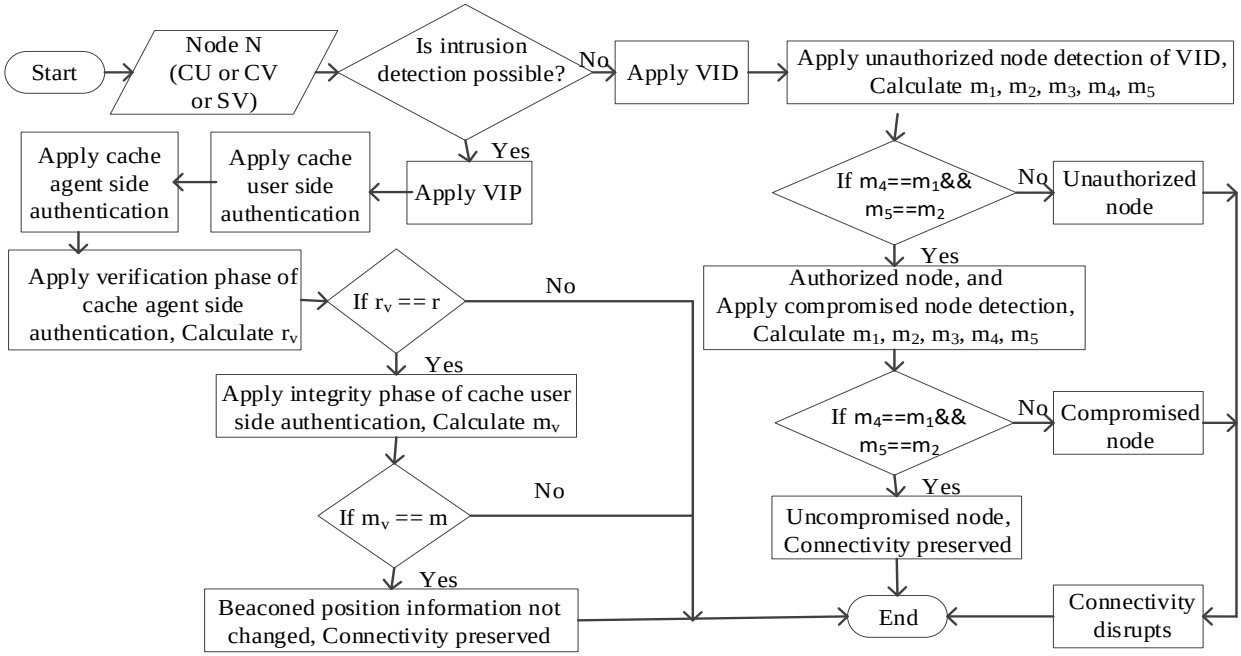


Fig.3. Vehicle Security Architecture of CMGV

The compromised node detection operates while hop-by-hop data dissemination. It is executed by vehicular infrastructure considering its vehicle monitoring capability due to the regularity or availability in the traffic environments. The detection is based on confidence interval calculation for next hop node using chi-square function. Considering X_1 as candidate next hop, and A, B as authenticated neighbors, the detection oriented message communication can be summarized as given by Eq. (17)-(21).

$$X_1 \rightarrow B, C: m_1 = {\beta_1}^{-x_1} {\beta_3}^{x_3} e^{f(x_1, x_2)} \quad (17)$$

$$B, C \rightarrow X_1: m_2 = H(\beta_1, \beta_3, x_1, x_3, m_1) \quad (18)$$

$$X_1 \rightarrow B, C: m_3 = \alpha_{14} - \alpha_5 + km_2(\alpha_9 - \alpha_{15}) + f(x_1, x_2) \quad (19)$$

$$B, C: m_4 = e^{m_3} \frac{({\beta_2}^{x_2} {\beta_4}^{x_4})^{km_2}}{({\beta_1}^{x_1} {\beta_3}^{x_3})^{km_2}} \quad (20)$$

$$B, C: m_5 = H(\beta_1, \beta_3, x_1, x_3, m_4) \quad (21)$$

Where β_i and α_i represent encryption parameters and Here, $f(x_1, x_2)$ denotes a chi-square distribution function. It is used to determine the confidence interval of sender node. Towards negating as a compromised node, the function value is considered under confidence interval once the constraints given by Eq. (22) and (23) satisfies.

$$m_4 = e^{m_3} \frac{({\beta_2}^{x_2} {\beta_4}^{x_4})^{km_2}}{({\beta_1}^{x_1} {\beta_3}^{x_3})^{km_2}} = {\beta_1}^{-x_1} {\beta_3}^{x_3} e^{f(x_1, x_2)} == m_1 \quad (22)$$

$$m_5 = H(\beta_1, \beta_3, x_1, x_3, m_4) = H(\beta_1, \beta_3, x_1, x_3, m_1) == m_2 \quad (23)$$

The next hop evaluation using confidence interval value validates a non-compromise node which can be used in data dissemination. The complete steps vehicular intrusion detection is presented as algorithm 2. The control flow architecture of CMGV framework is also presented in fig.3**.** It consists of VIP and VID techniques against cyber attacks in connected vehicle environments. In case of intrusion detection is not possible then, a VIP technique is applied using two-way authentication at network initialization stage namely, cache-user side authentication and cache-agent side authentication. Otherwise, a VID technique is applied focusing on next hop verification using unauthorized node detection and compromised node detection.

IV. Simulation Results and Performance Analysis

In this section, simulations carried out to evaluate the performance of the proposed vehicle cybersecurity framework for geocasting is discussed focusing on simulation settings, performance metrics, and comparative analysis.

A. *Simulation Settings*

The proposed CMGV framework is implemented in a vehicular traffic embedded and highly sophisticated ad-hoc network communication testbed, named CA-VANSL (Cache Agent based Vehicular Ad-hoc Networks Simulation Lab). This test bed is established in Communication Networks and Simulation Research Lab, School of Computer and Systems Sciences (SC&SS), Jawaharlal Nehru University (JNU), New Delhi, India. This testbed has effectively simulated a number of our previous research works [15], [16]. CMGV is simulated using Network Simulator (ns 2.35). Topologically Integrated Geographic Encoding and Referencing (TIGER) database is used for street layouts implementation in the proposed protocol [26]. The US Census Bureau Department for analyzing geospatial attributes of a region utilizes this database. Traffic simulator: Simulation for Urban Mobility (SUMO) is used for analyzing the distribution of vehicular nodes in different photo-periods [27].

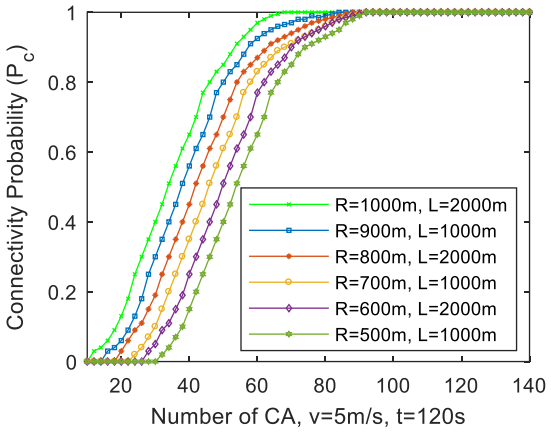
VanetMobiSim, an advanced version of CANU mobility simulation environment is used for generating realistic mobility patterns [28]. The main motive for optimal utilization of VanetMobiSim is due to the availability of both macro and micro mobility patterns. Intelligent-Driver Model is used for the management of node's movement in urban VANETs [29]. The performance of CMGV is compared with the state of the art techniques CTRC [13], D-Flooding [30], CAG [15], respectively. Table II shows the list of parameters used to configure the simulation scenario. The effectiveness of CMGV framework is measured using three different types of malicious vehicles. The type 1 malicious vehicles are prevented to join the network. The type 2 malicious vehicles are able to penetrate the secured architecture and are detectable. The type 3 malicious vehicles neither prevent to join the network nor detectable. The simulation result for every scenario is obtained by averaging results of 20 simulation repetitions with different seeds.

Table III. Simulation parameters

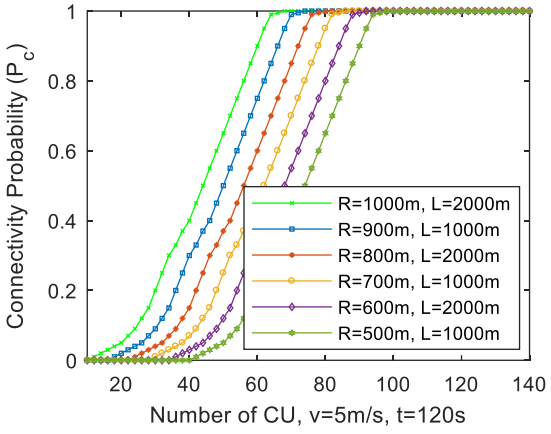
Parameter	Value	Parameter	Value
Mobility Model	$VanetMobiSim$	MAC protocol	802.11 DCF
Simulation Time	300 sec	Channel Capacity	4 $Mbps$
Map Size	1500 X 1500 m^2	Traffic Model	16 CBR
No .of Lanes	2 $lanes/dir$	Traffic light period	50 sec
No. of vehicles	500	Beaconing interval	0.75sec
Malicious vehicles	50	Packet senders	20
Velocity	$10-150km/hr$	Packet Type	UDP
Size of Buffer	64 KB	Channel Type	$Wireless$
Size of Packet	512 $Bytes$	Propagation Model	$Shadowing$
No. of Intersections	35	Antenna Model	$omnidirectional$
Transmission Range	500m to 1000m	Packet Rate	0.1 to 1 sec

B. *Analysis of Results*

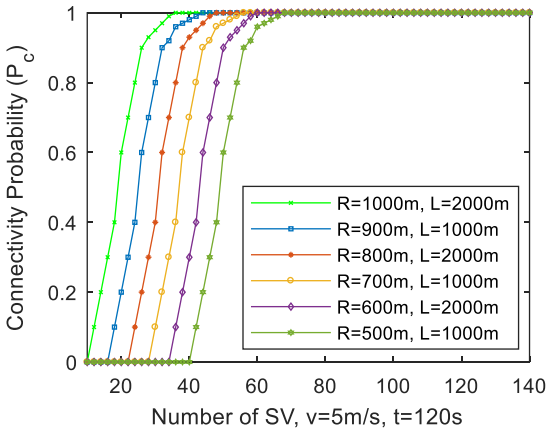
Two scenarios are considered to measure the impact of fixed and varying number of malicious vehicles on connectivity. Fig. 5 shows the relationship between connectivity probability and number of CU, CA and SV (fig. 4(a), 4(b), and 4(c)) respectively. As expected, for all the three cases, the connectivity probability increases as number of vehicles (CU or CA or SV) increase. The connectivity probability at high transmission range is higher as compared to the connectivity probability at low transmission range. CA achieves complete connectivity with lesser number of vehicles as compared to CU, since CA has higher transmission range as compared to CU. Similarly, SV has higher transmission range as compared to CA/CU, therefore achieves complete connectivity with lower number of vehicles. The number of vehicles per segment length to achieve desire level of connectivity can be precisely expected.



(a)



(b)



(c)

Fig.4. Connectivity Probability (P_C) vs Number of CA, CU and SV

Fig.5 shows the impact of malicious vehicles on the connectivity in case of CMGV and state-of-the-art techniques. In this simulation, 200 vehicles are considered. It is clearly enunciated that connectivity of CMGV steadily decreases as the

number of malicious vehicles increases. But connectivity in case of CAG, CTRC, and D-Flooding decreases gradually with lesser number of malicious vehicles, while decreases rapidly with large number of malicious vehicles. More specifically, for CMGV, the connectivity probability is in the range of 0.9-1.0, whereas it is 0.7-0.9, 0.6-0.2 and 0.4-0.02 in case of CAG, CTRC, and D-Flooding, respectively. This can be attributed to the fact that, in case of CMGV, VIP identifies the fake-beaconed position information and resists the intruder to join the network. If the malicious attacker is able to penetrate the secured architecture and compromises an insider, then VID phase is able to detect and block both malicious vehicles.

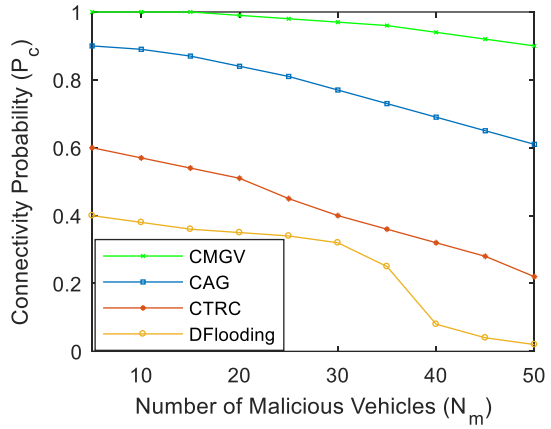


Fig.5. Connectivity Probability (P_C) vs Number of Malicious Vehicles (N_m)

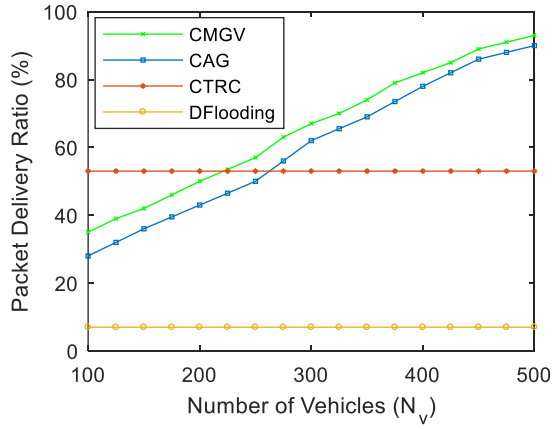


Fig. 6. Packet Delivery Ratio (%) vs Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

Fig.6 shows the packet delivery ratio with different values of the number of three types of vehicles N_V. It is clearly enunciated that packet delivery ratio of CMGV, and CAG steadily increases in commensurate with the increase of number of vehicles, while for CTRC, and D-Flooding, it remains constant. More specifically, in case of CMGV, packet delivery ratio is in the range of 35%-93%, whereas it is 30%-92%, 53% and 7% in case of CAG, CTRC, and D-Flooding, respectively. This can be attributed to the fact that, in case of CMGV, VIP phase identifies the fake beaconed position information and resists the intruder to join the network. If the malicious attacker is able to penetrate the secured architecture and compromises an insider, then VID phase is able to detect and block both malicious node and compromised node. CTRC has better packet delivery ratio as compared to D-flooding, due to utilization of caching methodology in case of unavailability of suitable nodes. D-flooding does not use caching technique in case of network fragmentation and has lowest packet delivery ratio.

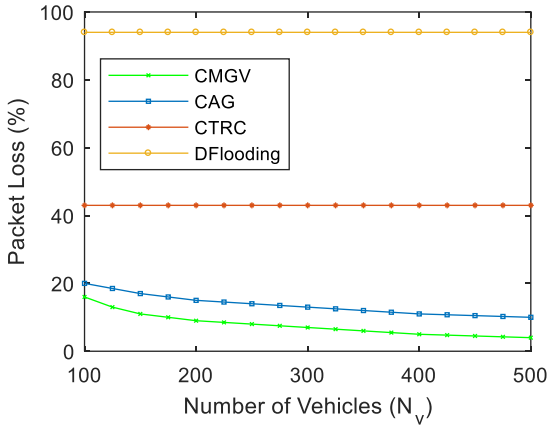


Fig. 7: Packet Loss (%) vs. Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

Fig.7 shows the packet loss with different values of number of vehicles (N_V). It clearly shows that the packet loss rate decreases, when number of vehicles increases in case of CMGV and CAG, and remains constant in case of CTRC, and D-flooding. In case of CMGV, utilization of VIP and VID helps in optimization of node selection process and chooses secure node as data forwarder. This minimizes the probability of packet loss. CAG utilizes CAA algorithm which reduces one hop transmission failure rate. The packet loss of CTRC is higher than CMGV and CAG, and not affected by the increment of N_V due to its non-usability of CAA algorithm, and non-consideration of off-road vehicles for data forwarding. The inability of delivering data packets in fragmented vehicular networks makes the packet loss highest in case of D- Flooding. In particular, for CMGV, packet loss rate is in the range of 20%-8%, whereas it is 20%-10%, 43% and 94% in case of CAG, CTRC and D-Flooding, respectively.

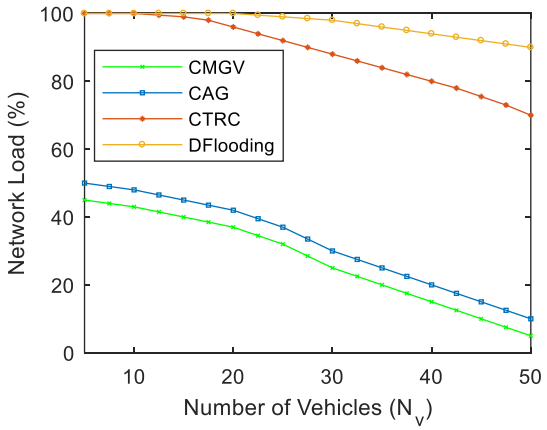


Fig. 8. Network Load (%) vs. Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

The results in Fig. 8 show the analysis of network load for data forwarding as a function of number of vehicles(N_V). It clearly shows that network load decreases with the increase of number of nodes. CMGV never uses flooding mechanism for data forwarding and chooses suitable NHV filtered by VIP and VID. It eliminates the probability of packet duplication. Both CTRC and D-flooding do not use any connectivity assurance methodology, therefore network load is very heavy initially. In particular, for CMGV, network load is in the range of 45-5, whereas it is 50-10, 100-70 and 100-90 in case of CAG, CTRC and D-Flooding, respectively.

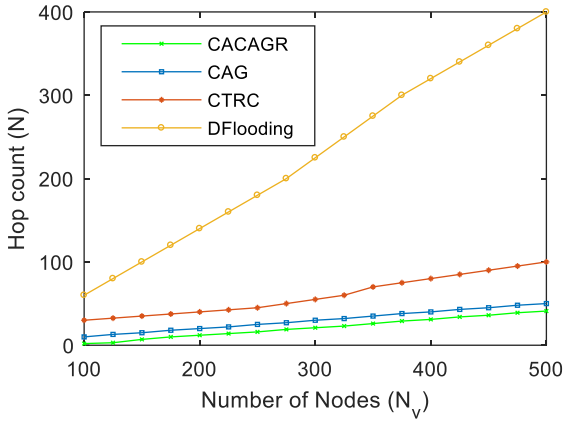


Fig. 9: Hop Count (N) vs. Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

Fig. 9 shows the variation in hop count with different values of number of vehicles(N_V). It clearly shows that enhancement in hop count is proportional to the number of vehicles. CMGV selects appropriate next hop vehicle using VIP and VID techniques, which reduces the hop count. CAG also shows less hop counts as it uses CAA algorithm integrated with most forwarding within radius (MFR). Though CTRC uses MFR techniques, it has no CAA mechanism, which enhances the one time transmission failure rate and results into more hop count. D-Flooding incorporates all vehicular nodes within the transmission range as suitable next hop vehicle, which results into the highest hop count. In particular, for CMGV, hop count is in the range of 2-41, whereas it is 10-50, 30-100 and 60-400 in case of CAG, CTRC and D-Flooding, respectively.

The results in Fig. 10 show the analysis of end-to-end delay as a function of number of vehicles(N_V). It clearly shows that the end-to-end delay reduces as number of vehicles increases. More specifically, for CMGV, end-to-end delay is in the range of 22-3, whereas it is 24-5, 33-25 and 36-21 in case of CAG, CTRC and D-Flooding respectively. CMGV minimizes the probability of one-hop connection failure as it uses a reliable path with the highest connectivity probability. The connectivity probability is high due to the selection of most trusted next hop vehicle filtered by VIP and VID phases. CTRC faces the problem of speed variation (when the intended next hop vehicle moves out of the transmission range of current forwarder) and increases the rate of one hop transmission failure. This results high end-to-end delay. D-flooding uses flooding technique, which increases the number of collisions.

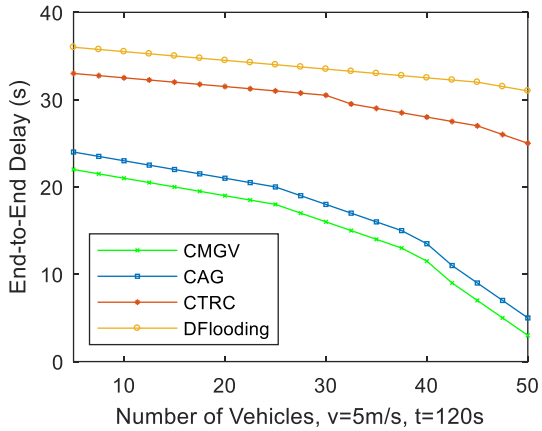


Fig. 10. End-to-End Delay (s) vs. Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

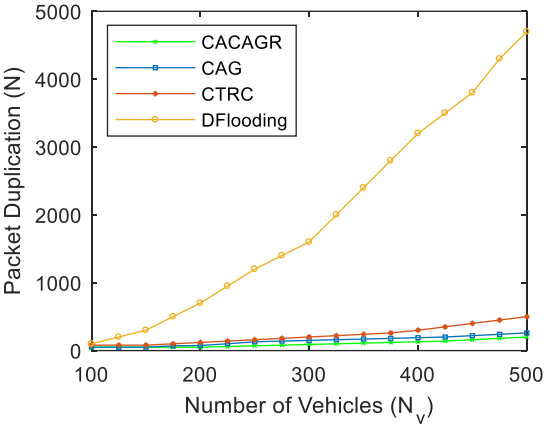


Fig. 11: Packet Duplication (N) vs Number of CA, CU and SV (N_V) in presence of 20 malicious vehicles

Fig. 11 shows variation in the packet duplication with the different values of number of vehicles(N_V). It clearly shows that the packet duplication is proportional to the number of vehicles. CMGV shows very low packet duplication rate as it prohibits the formation of duplicate packets by optimizing the selection of NHV. The malicious attacker is unable to masquerade the secured network and unable to form duplicate packets due to screening by VIP and VID phases. More specifically, for CMGV, packet duplication is in the range of 50-200, whereas it is 50-260, 80-500 and 100-4700 in case of CAG, CTRC and D-Flooding, respectively. The packet duplication rate in case of CAG is low due to its unique CA selection approach. CTRC has higher retransmission rate, which results into higher packet duplication rate. D-Flooding has the highest packet duplication rate as it totally depends on duplicate packets, generated due to flooding for its data delivery.

V. Conclusion and Future Work

In this paper, we have proposed a framework of cybersecurity measures for geocasting in vehicular cyber physical environment (CMGV). We determine the probability of connectivity of vehicular nodes for V2V and V2I communicational patterns. Connectivity oriented security measures: VIP and VID are developed to protect and defend the

connected vehicles. The simulation results validate that CMGV outperforms state of the art geocasting approaches in presence of malicious vehicles. The probability of connectivity rapidly increases for CMGV in commensurate with the increase of number of vehicular nodes, transmission range and types of vehicle. The packet delivery ratio, packet duplication, and hop count of CMGV increase, whereas packet loss rate, end-to-end delay and network load decrease in commensurate with the increase of number of vehicular nodes. In future research, authors will analyze the impact of traffic signal on connectivity by securing the traffic system and will investigate the security aspects by incorporating traffic load with the quality model and integrate our proposed concept with multilane highways.

APPENDIX-I

At first, the node X_1 sets $Y_{ii} = 0$. Then, it calculates Y_{ij} as follows.

$$Y_{ij} = y_i + y_j$$

$$Y_{ij} = ln\left(\beta_i^{x_i}\beta_j^{x_j}\right)$$

In this manner, all possible values of Y_{ij} are calculated. It is seen that $Y_{ij} = Y_{ji}$. The calculated values of Y_{ij} are given in Table III. The node X_1 calculates α_1 as follows.

$$\alpha_1 = Y_{12} + Y_{13}$$
$$= ln(\beta_1^{x_1}\beta_2^{x_2}) + ln(\beta_1^{x_1}\beta_3^{x_3})$$
$$= ln\left(\beta_1^{2x_1}\beta_2^{x_2}\beta_3^{x_3}\right)$$

In this manner, the node X_1 calculates different possible values of α_i as shown in Table IV.

TABLE I: calculation of Y_{ij}

Y_{ij}	1	2	3	4
1	0	$\ln(\beta_1^{x_1}\beta_2^{x_2})$	$\ln(\beta_1^{x_1}\beta_3^{x_3})$	$\ln(\beta_1^{x_1}\beta_4^{x_4})$
2	$\ln(\beta_1^{x_1}\beta_2^{x_2})$	0	$\ln(\beta_2^{x_2}\beta_3^{x_3})$	$\ln(\beta_2^{x_2}\beta_4^{x_4})$
3	$\ln(\beta_1^{x_1}\beta_3^{x_3})$	$\ln(\beta_2^{x_2}\beta_3^{x_3})$	0	$\ln(\beta_3^{x_3}\beta_4^{x_4})$
4	$\ln(\beta_1^{x_1}\beta_4^{x_4})$	$\ln(\beta_2^{x_2}\beta_4^{x_4})$	$\ln(\beta_3^{x_3}\beta_4^{x_4})$	0

TABLE II : Calculation of α_i

$\alpha_1 = Y_{12} + Y_{13} = \ln\left(\beta_1^{2x_1}\beta_2^{x_2}\beta_3^{x_3}\right)$	$\alpha_2 = Y_{12} + Y_{14} = \ln\left(\beta_1^{2x_1}\beta_2^{x_2}\beta_4^{x_4}\right)$	$\alpha_3 = Y_{12} + Y_{23} = \ln\left(\beta_1^{x_1}\beta_2^{2x_2}\beta_3^{x_3}\right)$
$\alpha_4 = Y_{12} + Y_{24} = \ln\left(\beta_1^{x_1}\beta_2^{2x_2}\beta_4^{x_4}\right)$	$\alpha_5 = Y_{12} + Y_{34} = \ln(\beta_1^{x_1}\beta_2^{x_2}\beta_3^{x_3}\beta_4^{x_4})$	$\alpha_6 = Y_{13} + Y_{14} = \ln\left(\beta_1^{2x_1}\beta_3^{x_3}\beta_4^{x_4}\right)$
$\alpha_7 = Y_{13} + Y_{23} = \ln\left(\beta_1^{x_1}\beta_2^{x_2}\beta_3^{2x_3}\right)$	$\alpha_8 = Y_{13} + Y_{24} = \ln(\beta_1^{x_1}\beta_2^{x_2}\beta_3^{x_3}\beta_4^{x_4})$	$\alpha_9 = Y_{13} + Y_{34} = \ln\left(\beta_1^{x_1}\beta_3^{2x_3}\beta_4^{x_4}\right)$
$\alpha_{10} = Y_{14} + Y_{23} = \ln(\beta_1^{x_1}\beta_2^{x_2}\beta_3^{x_3}\beta_4^{x_4})$	$\alpha_{11} = Y_{14} + Y_{24} = \ln\left(\beta_1^{x_1}\beta_2^{x_2}\beta_4^{2x_4}\right)$	$\alpha_{12} = Y_{14} + Y_{34} = \ln\left(\beta_1^{x_1}\beta_3^{x_3}\beta_4^{2x_4}\right)$
$\alpha_{13} = Y_{23} + Y_{24} = \ln\left(\beta_2^{2x_2}\beta_3^{x_3}\beta_4^{x_4}\right)$	$\alpha_{14} = Y_{23} + Y_{34} = \ln\left(\beta_2^{x_2}\beta_3^{2x_3}\beta_4^{x_4}\right)$	$\alpha_{15} = Y_{24} + Y_{34} = \ln\left(\beta_2^{x_2}\beta_3^{x_3}\beta_4^{2x_4}\right)$

REFERENCES

[1] Armstrong, L.; Fisher, W. IEEE 802.11P Wireless Access for Vehicular Environment, Drafts Standard. Available online: http://grouper.ieee.org/groups/802/11/

[2] O. Kaiwartya et al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," in IEEE Access, vol. 4,pp. 5356-5373, 2016.

[3] S. Al-Sultan, M. Al-Doori, A. H. Al-Bayatti, & H. Zedan, "A comprehensive survey on vehicular Ad Hoc network" Journal of Network and Computer Applications, Elsevier, 37(1), pp. 380-392, 2014.

[4] Schoitsch E., Schmittner C., Ma Z., Gruber T. (2016) The Need for Safety and Cyber-Security Co-engineering and Standardization for Highly Automated Automotive Vehicles. In: Schulze T., Müller B., Meyer G. (eds) Advanced Microsystems for Automotive Applications 2016. Lecture Notes in Mobility. Springer, Cham

[5] P. Papadimitratos et al., "Secure vehicular communication systems: design and architecture," in IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008.

[6] Levent Ertaul, Sridevi Mullapudi, "The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations." ICWN, pp. 3-9, 2009

[7] Kaiwartya, O. & Kumar, S. Wireless Pers Commun (2015) 83: 2657. https://doi.org/10.1007/s11277-015-2562-4.

[8] Kaiwartya, O.; Kumar, S.; Lobiyal, D.K.; Abdullah, A.H.; Hassan, A.N. Performance Improvement in Geographic Routing for Vehicular Ad Hoc Networks. Sensors 2014, 14, 22342-22371.

[9] Cao, Y., Han, C., Zhang, X., Kaiwartya, O., Zhuang, Y., Aslam, N. and Dianati, M., 2018. A Trajectory-Driven Opportunistic Routing Protocol for VCPS. IEEE Transactions on Aerospace and Electronic Systems.

[10] Grover, J., Laxmi, V. and Gaur, M.S., 2013. Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks. CSI transactions on ICT, 1(3), pp.261-279.

[11] Monteiro, M.E.P., Rebelatto, J.L. and Souza, R.D., 2016. Information-theoretic location verification system with directional antennas for vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 17(1), pp.93-103.

[12] Sheet, D.K., Kaiwartya, O., Abdullah, A.H., Cao, Y., Hassan, A.N. and Kumar, S., 2016. Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks. IET Intelligent Transport Systems, 11(2), pp.53-60.

[13] Maihofer, C. and Eberhardt, R. (2004) 'Geocast in vehicular environments: caching and transmission range control for improved efficiency (CTRC)', Intelligent Vehicles Symposium, IEEE, pp.951–956.

[14] Hassan, A.N., Abdullah, A.H., Kaiwartya, O. et al. Wireless Netw (2017). https://doi.org/10.1007/s11276-017-1502-5.

[15] Kaiwartya, Omprakash, and Sushil Kumar. "Cache agent-based geocasting in VANETs." International Journal of Information and Communication Technology 7.6 (2015): 562-584.

[16] R. Kasana *et al*., "Fuzzy based Channel Selection for Location Oriented Services in Multichannel VCPS Environments," in *IEEE Internet of Things Journal*. doi: 10.1109/JIOT.2018.2796639.

[17] Qing Yang, Alvin Lim, Shuang Li, Jian Fang and Prathima Agrawal, "ACAR: Adaptive Connectivity Aware Routing for Vehicular Ad Hoc Networks in City Scenarios,"Mobile Networks and Applications, Volume-15, pp: 36-60,2010..

[18] R. Kasana, S. Kumar, O. Kaiwartya, W. Yan, Y. Cao and A. H. Abdullah, "Location error resilient geographical routing for vehicular ad-hoc networks," in *IET Intelligent Transport Systems*, vol. 11, no. 8, pp. 450-458, 10 2017.

[19] K. Rabieh, M. M. E. A. Mahmoud and M. Younis, "Privacy-Preserving Route Reporting Schemes for Traffic Management Systems," in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2703-2713, March 2017.

[20] S. Yan, R. Malaney, I. Nevat and G. W. Peters, "Optimal Information-Theoretic Wireless Location Verification," in *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3410-3422, Sept. 2014.

[21] O. Abumansoor and A. Boukerche, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET," in *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275-285, Jan. 2012.

[22] M. Fogue *et al*., "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2538-2550,

June 2015.
[23] D. Ma, G. Tsudik, “Security and Privacy in Emerging Wireless Networks”, IEEE Wireless Communications, Vol 17, Issue 5, pages 12-21, 2010
[24] J. Kong et al., Adaptive security for multi-layer ad-hoc networks, Special Issue of Wireless Communications and Mobile Computing, John Wiley InterScience Press, 2002; 2:533–547.
[25] Baber Aslam, Soyoung Park, Cliff C. Zou,, Damla Turgut, “Secure traffic data propagation in Vehicular Ad Hoc Networks” International Journal of Ad Hoc and Ubiquitous Computing, Vol. 6, no. 1, pp. 24-39, 2010.
[26] J Sperling, Development and maintenance of the TIGER database: experiences in spatial data sharing at the US Bureau of the Census, in Proceedings of the Sharing Geographic Information (Centre for Urban Policy Research, New Brunseick, 1995), pp. 377-396
[27] Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz, “SUMO – Simulation of Urban Mobility”, in Proceedings of the 3rd International Conference on Advances in System Simulation (SIMUL 2011).
[28] J Harri, F Filali, C Bonnet, M Fiore, VanetMobiSim: generating realistic mobility patterns for VANETs, in Proceedings of the 3rd international workshop on Vehicular adhoc networks, VANET’06 (ACM, New York, NY, USA, 2006), pp. 96-97.
[29] D Tian, K Shafiee, VCM Leung, Position-based directional vehicular routing, in Proceeding of the Global Telecommunications Conference, GLOBECOM (IEEE, Hoboken, 2009), pp. 1-6.
[30] Sangho, O., Jaewon, K. and Gruteser, M. (2006) ‘Location-based flooding techniques for Vehicular emergency messaging (D-Flooding)’, Mobile and Ubiquitous Systems: Networking & Services, Third Annual International Conference on, pp.1–9, Springer.